Notice of Allowability	**Application No.** 09/884,672	**Applicant(s)** NOGUCHI ET AL.	
	Examiner Peter Poltorak	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment filed on 12/21/06 and an interview on 1/31/07 with Anne Dougherty.*.

2. ☒ The allowed claim(s) is/are *1,9-13,15,18,20-24,37,38,40 and 41*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

KAMBIZ ZAND
PRIMARY EXAMINER

DETAILED ACTION

1. This Office Action is in response to Applicant's amendment filed on 12/21/06 and the examiner initiated interview conducted on 1/31/07.

Allowable Subject Matter

2. In light of the discussion with applicant's representative, applicant's amendment and amendments to claims 1, 9-13, 15, 18, 20-24, 37-38 and 40-41, these claims are allowed.

Examiner Amendment

3. An Examiner's Amendment to the record appears below. Should the changes and/or additions be unacceptable to Applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the Issue Fee.

The following changes were authorized (and permission to make same by Authorization for this Examiner's Amendment was given in a telephone interview with Anne Dougherty on 1/31/07.

Please cancel claims 2-7, 16 and 19,

and replace claim 1 as follows:

--

An ad-hoc radio communication verification system, comprising:

~~means~~ a section sending data for verification data generation from a first data send/receive device to a second send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection;

in the first data send/receive device, ~~means~~ a section ~~for~~ generating verification data from the sent data for verification data generation produced using a first generation algorithm, for ~~and~~ outputting the generated first verification data to a first verification data output section and for communicating said first verification data to said second data send/receive device;

in the second data send/receive device, ~~means~~ a section ~~for~~ generating verification data from the received data for verification data generation produced using the first generation algorithm, for ~~and~~ outputting the generated second verification data to a second verification data output section and for communicating said second verification data to said first send/receive device; and

~~means~~ a section ~~for~~ at each of said first and second send/receive devices for determining whether the verification data at the first and second verification data output sections matches mutually,

wherein the first generation algorithm generates a plurality of verification data, wherein for each verification data, it is determined whether the verification data at the first and second verification data output sections match mutually;

a section establishing a serial sequence of operators that are composed of two or more of operators arranged in series, wherein the operators relate to the same or different one-way functions; and

a section letting an input to the serial sequence of operators be the data for verification data generation and outputs of two or more of operators selected from all operators composing the serial sequence of operators or corresponding values be the verification data respectively;

and

wherein said section determining for each verification data whether the verification data match mutually at the first and second verification data output sections comprises a section for comparing sequences of verification data.

--

Please replace claim 9 as follows:

--

An ad-hoc radio communication data send/receive system utilizing the ad-hoc radio verification system according to ~~claim 8~~ claim 1, comprising:

for each user, a portable terminal having a radio communication function and a personal computer having a radio communication function, wherein the portable terminal and personal computer of each user are connected by a secure communication path; and wherein each portable terminal comprises a transmission section ~~means~~ whereby a public key Kp of a first user is transmitted from the portable terminal of the first user to the portable terminal of a second user without being tampered with, as determined by the ad-hoc radio communication system, and the public key Kp is transmitted from the portable terminal to the personal computer of each user, and wherein each personal computer comprises a section ~~means~~ to generate a symmetric key Kc such that the personal computer of the second user generates a symmetric key Kc produced using a second generation algorithm, while the personal computer of the first user generates the symmetric key Kc produced using the second generation algorithm from information including a random number and an identifier for the second generation algorithm transmitted from the personal computer of the second user in cipher using the public key and deciphered at said personal computer of the first user; and thereafter both the personal computers send and receive data in cipher using the symmetric key Kc.

--

Please replace *the first three lines* of claim 10 with:

--

An ad-hoc radio communication

data send/receive system utilizing the ad-hoc radio

communication verification system according to claim ~~8~~ 1,

--

and *line 13* (of claim 10) with:

--

each personal computer comprises a section ~~means~~ to generate

--

Please replace claim 11 *line 17* (which is line 3 on page 8) with:

--

personal computer comprises a section ~~means~~ to generate a

--

Please replace claim 13 as follows:

--

A method for verifying an ad-hoc radio communication, comprising the steps of:

sending data for verification data generation from a first data send/receive device to a second send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection;

in the first data send/receive device, generating verification data from the sent data for verification data generation produced using a first generation algorithm and outputting the generated first verification data to a first verification data output section and communicating said first verification data to said second data send/receive device;

in the second data send/receive device, generating verification data from the received data for verification data generation produced using the first generation algorithm and outputting the generated second verification data to a second verification data output section and communicating said second verification data to said first send/receive device; ~~and~~

determining at each of said first and second send/receive devices whether the verification data at the first and second verification data output sections match mutually;

establishing a serial sequence of operators that are composed of more than one operators arranged in series, wherein the operators relate to the same or different one-way functions; and

letting an input to the serial sequence of operators be the data for verification data generation and an output from the serial sequence of operators or a corresponding value be the verification data.

--

Please replace claim 18 as follows:

--

The method according to claim 13 further comprising ~~the steps of;~~

~~establishing a serial sequence of operators that are composed of two or more of operators arranged in series wherein the operators relate to the same or different one-way functions;~~

~~letting an input to the serial sequence of operators by the data for verification data generation and outputs of two or more of operators selected from all operators composing the serial sequence of operators or corresponding values be the verification data respectively; and~~

determining for each verification data whether the verification data match mutually at the verification data output sections of both the data send/receive devices.

--

Please replace claim 37 as follows:

--

An article of manufacture comprising a computer usable medium having computer readable program code ~~means~~ embodied therein for causing ad-hoc radio communication, the computer readable program code ~~means~~ in said article of manufacture comprising computer readable program code ~~means~~ for causing a computer to effect the steps of claim 13.

--

Please replace claim 38 as follows:

--

An article of manufacture comprising a computer usable medium having computer usable medium having computer readable program code ~~means~~ embodied therein for causing ad-hoc radio communication, the computer readable program code ~~means~~ in said article of manufacture comprising computer readable program code ~~means~~ for causing a computer to effect the steps of claim 21.

--

Please replace claim 40 as follows:

--

An article of manufacture comprising a computer usable medium having computer readable program code ~~means~~ embodied therein for causing ad-hoc radio communication, the computer readable program code ~~means~~ in said article of manufacture comprising computer readable program code ~~means~~ for causing a computer to effect the steps of claim 23.

--

Please replace claim 41 as follows:

--

An article of manufacture comprising a computer usable medium having computer readable program code ~~means~~ embodied therein for causing ad-hoc radio communication, the computer readable program code ~~means~~ in said article of manufacture comprising computer readable program code ~~means~~ for causing a computer to effect the steps of claim 24.

--

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on statement of Reasons for Allowance”.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached from Monday through Thursday from 9:00 until 5:00, and every other Friday from 9:00 until 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (571) 272-1600.

3/1/07

KAMBIZ ZAND
PRIMARY EXAMINER